UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re Pork Antitrust Litigation This Document Relates To All Actions	Case No. 18-cv-01776-JRT-HB

DECLARATION OF AMY MORRISON

I, Amy Morrison, declare as follows:

1. I am over the age of eighteen and make this declaration based upon my personal knowledge.

2. My current position is Director of Infrastructure Services at Hormel Foods Corporation ("Hormel Foods").

3. I became the Manager of Infrastructure Services in 2013 and the Director of Infrastructure Services on May 9, 2016.

4. Hormel Foods' Bring Your Own Device ("BYOD") program, established in 2011, allows employees to interact remotely with a subset of Hormel Foods' corporate systems using their personally-owned mobile device and is governed by Hormel Foods' Mobile Device Policy ("MDP").

5. I am the policy owner of Hormel Foods' MDP and have responsibility for review and maintenance of the policy.

6. The MDP's provisions have been consistent throughout the years, with minor changes to reimbursement policies and to accommodate changes in platforms supported.

7. Hormel Foods owns all data that is sourced from Hormel Foods' systems and synched between the mobile device and its servers.

8. That data primarily consists of company email, calendars, and contacts (if set up through an employee's corporate email account).

9. This data does not include text messages or other information on a personally-owned device, such as photos or personal application data.

10. The MDP has consistently provided that "devices are owned by the employee, and the employee is solely responsible for all immediate and future costs associated with the purchase of the mobile device and accessories." *See* MDP § B.

11. The MDP permits Hormel Foods to retire (remove) MobileIron and MobileIron-controlled data or to initiate a remote wipe (factory reset) of enrolled employees' devices using the MobileIron software when necessary to protect Hormel Foods' data from risk of misappropriation or other use. *Id.* § F.

12. A remote wipe will delete all data on the mobile device that has not been previously backed-up or synchronized by the device owner using a device management account.

13. A device management account (such as iTunes, iCloud, or Google Drive) allows device owners to maintain and backup personal information including text messages, photos, and personal application data.

14. Hormel Foods employees enrolled in the BYOD program cannot, however, use a device management account to back up data owned by Hormel Foods or used in connection with any applications delivered by Hormel Foods via MobileIron.

15. The MDP provides that the "employee is responsible for the device management account." *Id.* § B.

16. The MDP further provides that "[a]ll app downloads and purchases for the device are the sole responsibility of the owner or assigned user of the device." *Id.*

17. In the event of a remote wipe, if device owners have elected to maintain a device management account and backed up their personal data, they may restore that data, including text messages, photos, and personal application data.

18. The MobileIron software which permits Hormel Foods to remotely wipe employees' personal devices does not allow Hormel Foods to access the personal content of employees, including:

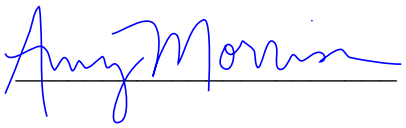
- Personal Email
- Text Messages
- Personal Contacts
- Device Location
- Photos and Videos
- Voicemail
- Content of Personal Applications

19. Hormel Foods does not have the technical ability to remotely "image" a phone.

20. Hormel Foods employees have never performed an "imaging" process to extract personal data from devices owned by other employees.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 31st day of August, 2021



Amy Morrison